WHAT IS CLAIMED IS:

1. A single sign-on authentication system, comprising:

an authentication component that determines whether a user is authenticated, and, if it is determined that the user is authenticated, generates a connection request;

an interface component that receives the connection request from the authentication component, the connection request including an identifier and entitlement information; wherein the interface component compares the received identifier with an expected identifier and, if they match, makes the entitlement information available to a server associated with the interface component.

2. The single sign-on authentication system of claim 1, wherein the entitlement information is different from information used to authenticate the user.

3. The single sign-on authentication system of claim 1, wherein the identifier includes an Internet Protocol (IP) address.

4. The single sign-on authentication system of claim 2, wherein the authentication component determines the entitlement information based on the information used to authenticate the user.

5. The single sign-on authentication system of claim 4, wherein the information used to authenticate the user includes one or more of a user identifier and a password.

6. The single sign-on authentication system of claim 1, wherein the entitlement information is contained in a header portion of a data packet.

7. The single sign-on authentication system of claim 1, wherein the connection request is sent as an HTTP request.

8. A method for enabling an authenticated user to connect to a server in a computer network, comprising:

receiving a connection request for the authenticated user, the connection request including an identifier and entitlement information;

comparing the received identifier with an expected identifier; and

making the entitlement information available to the server, only if the result of the comparison is a match.

9. The method of claim 8, wherein the entitlement information is different from information used to authenticate the authenticated user.

10. The method of claim 8, wherein the received identifier includes an Internet Protocol (IP) address.

11. The method of claim 9, wherein the entitlement information is determined based on the information used to authenticate the user.

12. The method of claim 11, wherein the information used to authenticate the authenticated user includes one or more of a user identifier and a password.

13. The method of claim 8, wherein the entitlement information is contained in a header portion of a data packet.

14. The method of claim 8, wherein the connection request is sent as an HTTP request.

15. A program storage device readable by a machine, tangibly embodying a program of instructions executable on the machine to perform method steps for enabling an authenticated user to connect to a server in a computer network, the method steps comprising:

receiving a connection request for the authenticated user, the connection request including an identifier and entitlement information;

comparing the received identifier with an expected identifier; and

making the entitlement information available to the server, only if the result of the comparison is a match.